USA Patriot Act Requires Banks To Implement Customer Identification Programs

The Department of the Treasury, together with the federal banking agencies (Agencies), have issued their jointly adopted final rule (Rule) to implement section 326 of the USA Patriot Act of 2001. That Act requires banks to implement a customer identification program (CIP) when accounts are opened. The CIP requires, at a minimum, reasonable procedures for (i) verifying the identity of any person seeking to open an account; (ii) maintaining records of the information used to verify the person's identity; and (iii) determining whether the person appears on any lists of known or suspected terrorists provided to the financial institution by any government agency. Although the Rule is effective as of May 30, 2003, the final compliance date for banks to implement a CIP is October 1, 2003 to allow time for banks to revise existing account opening policies and procedures, obtain board approval, train staff, update forms, purchase customer verification software and purchase new equipment for storing records.

What is Covered under Rule

The Rule applies to those accounts, both consumer and commercial, in which a formal banking relationship has been established. Infrequent transactions, such as an occasional wire transfer, are not considered accounts under the Rule. The Rule contains a "transfer exception" which excludes from the definition of accounts those accounts a bank acquires through an acquisition, merger, purchase of assets or assumption of liabilities from a third party. The Rule defines "customer" to mean a person that opens a new account. "Customer" does not include a signatory to an account, nor certain readily identifiable entities, such as publicly traded companies, but only to the extent of their domestic operations. However, the requirements of the Act are merely minimum requirements. A bank should include in its CIP those situations when it needs to take additional steps to verify the identity of a non-individual customer, including seeking information on individuals who control an account, such as signatories.

Customer Identification Program Requirements

The Rule requires that a bank's CIP contain procedures that specify the identifying information that the bank must obtain from each customer prior to opening an account. These include name, date of birth (for an individual), address and identification number. However, based upon an assessment of risks, a bank may require a customer to provide additional information to establish the customer's identity in order for the bank to establish a reasonable belief it knows the true identity of the customer.

The Rule provides that a bank generally must obtain a residential or business street address for a customer who is an individual. The Agencies felt that it was important for law enforcement agencies to be able to contact a customer at a physical location. The Rule contains limited exceptions for individuals who cannot readily provide a physical address, allowing, for example, a bank to obtain an Army Post Office box number, or the residential or business street address of next of kin.

The Rule requires banks to obtain an identification number from every customer opening an account. For U.S. persons, that identifying number must be a social security number or a taxpayer identification number (TIN). There are no exceptions. Agency guidance on the implementation of the Rule has indicated that even members of sects, such as the Amish, that do not want to be identified by a number, still will be required to

provide a social security number at account opening. As to the timing of obtaining the identification number, the Rule provides that in those circumstances in which a person has applied for, but has not yet received a TIN, a bank's CIP may provide for procedures to confirm that the TIN has been applied for and that the TIN is received within a reasonable period of time after the account is opened.

Because there is no uniform identification number that non-U.S. persons are able to provide to a bank, a bank has the option to obtain a variety of identification numbers from non-U.S. persons, including passport numbers and country of issuance and alien identification numbers. A bank must decide for itself, based upon appropriate risk factors, whether the information presented by the customer enables the bank to establish a reasonable belief that it knows the true identity of the customer.

The Rule requires that bank's CIP contain procedures for identity verification. Verification may be through such things as an unexpired driver's license or passport. For an entity, verification may include things such as certified articles of incorporation, a partnership agreement or a trust instrument. For those accounts that are opened by telephone, mail or over the Internet, a CIP must contain procedures that describe the methods the bank will use to verify identification. Acceptable verification methods include contacting a customer, or independently verifying the customer's identity by comparing information provided by the customer with that obtained from a consumer reporting agency.

Recordkeeping and Record Retention Requirements

CIPs must include procedures for making and maintaining a record of the identifying information, a description of any documents relied upon (including type of document, identification number, place of issuance, and if any, date of issuance and expiration date) a description of the methods used to verify the identity and a description of the resolution of any discrepancy. The identifying information must be retained for five years after the date the account is closed, or in the case of credit card accounts, five years after the account is closed or becomes dormant. All other information required by the CIP must be retained for five years after the record is made.

Comparing with Government Lists of Known or Suspected Terrorists

CIPs must include procedures for determining whether the customer appears on any list of known or suspected terrorists or terrorist organizations issued by any Federal government agency within a reasonable time after the account is opened, if not earlier required by another Federal law or directive. The Agencies have noted that lists that banks must check in order to comply with this provision have not yet been designated, and therefore, as yet, banks do not have an affirmative duty to seek out all lists of known or suspected terrorists for purposes of their CIP. Banks will receive notification by way of separate Agency guidance regarding the lists to be consulted.

Susan B. Hollinger is admitted in New Hampshire and Massachusetts.

Gallagher, Callahan & Gartrell
Copyright May 2003

Reprinted by permission